Hardware Implementations of NIST Lightweight Cryptographic Candidates: A First Look

Behnaz Rezvani
William Diehl

Bradley Dept. of Electrical and Computer Eng.
Virginia Tech
Blacksburg, Virginia

November 5, 2019
Outline

- Introduction
- Rationale of selecting Ciphers
- FPGA Implementations
  - SpoC
  - Spook
  - GIFT-COFB
  - CAESAR LW API
- Results
- Conclusions
Introduction

- Devices in IoT are vulnerable to theft of privacy information and are subject to potentially more destructive attacks

- Conventional methods of security provisions:
  - Encryption/Decryption → Confidentiality
  - MAC → Authentication
  - Hash → Data integrity

- AEAD combines confidentiality, data integrity, and authentication into a single algorithm
  - Savings in cost and performance
  - Good for lightweight applications
  - But, more complex security analysis
Round 1 Candidates

- **Functionality:**
  - AEAD (34)
  - AEAD + Hash (22)

- **Block cipher or permutation-based** (51) vs. stream cipher and others (5)
  - Permutation-based (26)

- **Permutation structures:** SPN (37), Feistel (10), 3D state (4), Misty (1), LS-design (1)

- **S-box:** 4-to-2-bit (1), 3-bit (1), 4-bit (22), 5-bit (5), 8-bit (12), 9-bit (1)

- **Non-linearity:**
  - AND (9)
  - ARX* (6)

*ARX: Addition, Rotation, XOR*
Rationale of Selection

- **Different structures:**
  - Block-based: GIFT-CO FB
  - Sponge-based: SpoC, Spook

- **Different permutation designs:**
  - sLiSCP-light permutation: SpoC
  - LS-design: Spook
  - SPN: GIFT-CO FB

- **Different types of confusion:**
  - S-box: Spook, GIFT-CO FB
  - AND: SpoC

- **Tweakable Block Cipher:**
  - Spook
SpoC Construction

- SpoC mode of operation:
  - Sponge with a masked capacity
  - Higher security
  - Larger rate value per permutation call

\[
\frac{f(N_0, K)}{b=192} \xrightarrow{N_1 \text{ c=128}} \xrightarrow{A_{a-1}} \xrightarrow{M_{m-1}} \text{Permutation} \xrightarrow{\text{tag} \text{ 64}} \]

sLiSCP-light
SpoC: sLiSCP-light[192]

- Combination of a type II generalized Feistel structure (GFS) and Simeck box
- 3 transformations in each step (18 steps)
  - SubstituteSubblocks (SSb) (6 rounds)
  - AddStep constants (ASC)
  - MixSubblocks (MSb)
SpoC Implementation

- 1 round of the SSb: 1 clock cycle
  - 108 clock cycles per permutation
- Initialization and Tag gen.: 219 CC
- Every block of AD: 109 CC
- Every block of M: 111 CC
- Requires 10\* padding
- Truncate the output (|CT|=|PT|)
- Primary member achieves Ciphertext Integrity and Misuse with Leakage in encryption and decryption (CIML2), which is an extension of ciphertext integrity in the presence of nonce misuse and side-channel leakages.
- Single one pass (S1P) mode of operation.
- Clyde-128: A tweakable LS-design (L-box, S-box).
- Shadow-512: A multiple LS-design (L-box, S-box, diffusion layer).
Spook Implementation

- 1 round of TBC: 1 clock cycle
  - 12 clock cycles per TBC
  - 144 clock cycles per permutation

- Initialization and Tag gen.: 169 CC
- Every block of AD: 145 CC
- Every block of M: 145 CC

- L-box and S-box are shared
- Requires 10 padding
- Truncate the output (|CT|=|PT|)
- Combined-feedback mode of operation
  - Single pass
  - Inverse free
- Underlying cipher: GIFT-128
GIFT-COFB Implementation

- 1 round: 1 clock cycle
  - 40 clock cycles per GIFT cipher
- Initialization and Tag gen.: 112 CC
- Every block of AD: 50 CC
- Every block of M: 53 CC
- Requires 10\(^*\) padding
- Truncate the output (|CT|=|PT|)
CAESAR LW API

- CAESAR LW developer's package:
  - Input processor (Pre-Processor)
  - Output processor (Post-Processor)
  - Designer’s cipher (CipherCore)
Implementation Setup

- Methodology ➔ RTL
- FPGA platform ➔ Artix-7
- Interface ➔ CAESAR hardware API (LW developer’s package)
- Operation tool ➔ Xilinx Vivado 2018.3
- Optimization tool ➔ Minerva automated hardware optimization tool
- Goal of optimization ➔ Throughput to area (TPA) ratio
- Test vector generator ➔ aeadtvgen in the developer’s package
- Verification hardware ➔ FOBOS

- All ciphers are implemented in basic iterative (round-based) architecture.
Benchmarking Results

- **Latency**: # of clock cycles to process one block of PT from start to end
- **Throughput**: 
  \[(\text{Max Freq}) \times (\text{Bits/Block})/(\text{Cycles/Block})\]
- **SpoC** has the highest frequency and smallest area.
- **GIFT-COFB** has the highest TP and TPA and the smallest latency.
- **Spook** has largest area but higher TP than **SpoC**.

<table>
<thead>
<tr>
<th>Cipher</th>
<th>SpoC</th>
<th>Spook</th>
<th>GIFT-COFB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Freq (MHz)</td>
<td>265</td>
<td>141</td>
<td>172</td>
</tr>
<tr>
<td>#Bits/Block</td>
<td>64</td>
<td>256</td>
<td>128</td>
</tr>
<tr>
<td>#Cycles/Block</td>
<td>111</td>
<td>145</td>
<td>53</td>
</tr>
<tr>
<td>Latency</td>
<td>330</td>
<td>314</td>
<td>165</td>
</tr>
<tr>
<td>Throughput (TP) (Mbps)</td>
<td>152.8</td>
<td>248.9</td>
<td>415.4</td>
</tr>
<tr>
<td>LUTs</td>
<td>1344</td>
<td>7082</td>
<td>2695</td>
</tr>
<tr>
<td>TPA (Mbps/LUT)</td>
<td>0.114</td>
<td>0.035</td>
<td>0.154</td>
</tr>
</tbody>
</table>
## Comparison

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Type</th>
<th>FPGA</th>
<th>Freq (MHz)</th>
<th>Area (LUTs)</th>
<th>TP (Mbps)</th>
<th>TPA (Mbps/LUT)</th>
<th>Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CAESAR</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ascon-128</td>
<td>Sponge</td>
<td>Spartan-6</td>
<td>216.0</td>
<td>684</td>
<td>60.1</td>
<td>0.088</td>
<td>Yalla et al.: Evaluation of the CAESAR Hardware API for Lightweight Implementations. 2017</td>
</tr>
<tr>
<td>Ascon-small</td>
<td>Sponge</td>
<td>Spartan-6</td>
<td>146.1</td>
<td>1640</td>
<td>114.0</td>
<td>0.070</td>
<td>Diehl et al.: Face-off between the caesar lightweight finalists: Acorn vs. ascon. 2018</td>
</tr>
<tr>
<td>CLOC-AES</td>
<td>Block</td>
<td>Spartan-6</td>
<td>101.9</td>
<td>1604</td>
<td>68.7</td>
<td>0.043</td>
<td>Farahmand et al.: Improved lightweight implementations of caesar authenticated ciphers. 2018</td>
</tr>
<tr>
<td>SILC-AES</td>
<td>Block</td>
<td>Spartan-6</td>
<td>115.1</td>
<td>872</td>
<td>15.1</td>
<td>0.017</td>
<td>Farahmand et al.: Improved lightweight implementations of caesar authenticated ciphers. 2018</td>
</tr>
<tr>
<td><strong>NIST LWC (AEAD)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SpoC</td>
<td>Sponge</td>
<td>Artix-7</td>
<td>265.0</td>
<td>1344</td>
<td>152.8</td>
<td>0.114</td>
<td>TW</td>
</tr>
<tr>
<td>Spook</td>
<td>Sponge</td>
<td>Artix-7</td>
<td>141.0</td>
<td>7082</td>
<td>248.9</td>
<td>0.035</td>
<td>TW</td>
</tr>
<tr>
<td>Spook</td>
<td>Sponge</td>
<td>Artix-7</td>
<td>181.8</td>
<td>3771</td>
<td>3878.4</td>
<td>1.028</td>
<td>Spook Team: Spook (unprotected) implementation of encryption. email of Jul. 30, 2019.</td>
</tr>
<tr>
<td>GIFT-COFB</td>
<td>Block</td>
<td>Artix-7</td>
<td>172.0</td>
<td>2695</td>
<td>415.4</td>
<td>0.154</td>
<td>TW</td>
</tr>
<tr>
<td>SAEAES</td>
<td>Block</td>
<td>Virtex-7</td>
<td>145.9</td>
<td>348</td>
<td>263.3</td>
<td>0.757</td>
<td>Naito, Y., Matsui, M., Sakai, Y., Suzuki, D., Sakiyama, K., Sugawara, T.: SAEAES (Feb 2019).</td>
</tr>
</tbody>
</table>
Power and Energy/Bit

- Power measured @ 10, 25, 50 MHz using FOBOS on Artix-7
- E/bit (nJ/bit) = \( P \) (mW)/TP(Mbps)
- Ascon has the lowest power at 50 MHz.
- GIFT-COFB has the lowest E/bit at 50 MHz.
- Spook has the highest power.

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Freq (MHz)</th>
<th>( P_{\text{mean}} ) (mW)</th>
<th>TP (Mbps)</th>
<th>E/bit (nJ/bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-GCM</td>
<td>10</td>
<td>28.6</td>
<td>6.2</td>
<td>4.59</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>31.4</td>
<td>15.6</td>
<td>2.01</td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>35.9</td>
<td>31.2</td>
<td>1.15</td>
</tr>
<tr>
<td>ASCON</td>
<td>10</td>
<td>28.1</td>
<td>7.8</td>
<td>3.60</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>30.3</td>
<td>19.5</td>
<td>1.55</td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>33.6</td>
<td>39.0</td>
<td>0.86</td>
</tr>
<tr>
<td>SpoC</td>
<td>10</td>
<td>28.6</td>
<td>5.8</td>
<td>4.96</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>30.8</td>
<td>14.4</td>
<td>2.14</td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>34.7</td>
<td>28.8</td>
<td>1.20</td>
</tr>
<tr>
<td>Spook</td>
<td>10</td>
<td>58.8</td>
<td>17.7</td>
<td>3.33</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>96.5</td>
<td>44.1</td>
<td>2.19</td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>125.9</td>
<td>88.3</td>
<td>1.43</td>
</tr>
<tr>
<td>GIFT-COFB</td>
<td>10</td>
<td>29.1</td>
<td>24.2</td>
<td>1.20</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>32.0</td>
<td>60.4</td>
<td>0.53</td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>36.6</td>
<td>120.8</td>
<td>0.30</td>
</tr>
</tbody>
</table>

- $P_{\text{static}}$ is estimated with linear interpolation.
- Static powers of all ciphers (except Spook) are 27.0mW±1%.
- The static power of Spook is much higher, likely due to its larger area.

Conclusions

- We provided the first look at 3rd-party FPGA implementations of selected NIST LWC standardization process Round 1 candidates.

- **SpoC** has the highest maximum frequency of 265 MHz (1.9 greater than Spook), and has the lowest area, in terms of LUTs, with 1344 LUTs (19% of the LUTs of Spook).

- **GIFT-COFB** has the highest throughput (TP) at 415.4 Mbps (2.7 greater than SpoC), the highest throughput-to-area (TPA) ratio at 0.154 Mbps/LUT (4.4 more than Spook), and the lowest energy/bit at 50 MHz.

- **Spook** has the highest area due to its security features that it guarantees, but can be implemented in leveled implementations to get smaller area and higher TP.
Thank you!